REMARKS

In the Office Action, the Examiner rejected Claims 13-20 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,355,474 (issued Oct. 11, 1994; hereafter "Fahlman") in view of U.S. Patent 5,960,080 (issued Sept. 28, 1999; hereinafter "Thuraisngham"). The Examiner also rejected Claim 30 under 35 U.S.C. § 103(a) as being unpatentable over Thuraisnghamin view of Fahlman. The Applicant respectfully traverses the rejections of Claims 13 – 20 and 30 and submits the following arguments. Additionally, the Applicant has added new Claims 31 - 34 and submits arguments in support of patentability.

Claims 13 - 20

In Claim 13, the Applicant recites a method for use in a multi-level secure system for sanitizing a message. The multilevel secure system includes at least first and second security levels with first security level users being authorized to receive sensitive information that second security level users are not authorized to receive. The method includes steps of establishing a computer-based sanitization tool for sanitizing messages based on predefined sanitization rules, using the computer-based sanitization tool to receive a message for potential distribution, and operating the computer-based sanitization tool to identify at least first and second potential recipients having first and second security clearances, respectively. For example, some users may be associated with a first security level whereas others are associated with a second security level that do not have access to certain information that the first security level users have. The method further includes a step of operating the computer-based sanitization tool to sanitize a received message and generate a first sanitized message for transmission to the first potential recipient. The method also includes a step of operating the computer-based sanitization tool for sanitizing the received message to generate a second sanitized message for transmission to the second potential recipient. This second message differs from the first sanitized message in that the first sanitized message contains information that the second potential recipient is not allowed to receive.

As the Examiner stated in previous Office Actions, Fahlman does not teach operating a computer-based tool for identifying first and second potential recipients having first and second security clearances, respectively. The Applicant agrees and further notes that Fahlman does not, in fact, teach using the computer-based tool to identify anyone. Nor does Fahlman teach operating a computer-based sanitization tool for sanitizing a received message to generate first and second sanitized messages that differ based on respective first and second security levels. Fahlman also does not teach first and second sanitized messages.

While Fahlman does not teach operating a computer-based tool for identifying first and second potential recipients having respective first and second security clearances, the Examiner states that Thuraisnghamin teaches such at column 8, lines 37 - 39. Thuraisnghamin merely states that "[t]he constraint manager, which is trusted, will ensure that a user can read the constraints classified only at or below his level." While such a statement may indicate that the constraint manager identifies security levels of certain files, it in no way indicates that the constraint manager identifies whether potential recipients have certain security levels. That is because the Thuraisnghamin teaches a database which stores information based on security levels such that users may access the database and retrieve information based on the user's security level. The configuration of the data base prevents people from accessing data that they are not entitled to view. This differs from the Applicant's claim because, among other reasons, Thuraisnghamin must rely on a user's login before releasing information as opposed to identifying a recipient entitled to receive information. *See e.g.*, column 4, lines 8 – 41 of Thuraisnghamin.

Fahlman and Thuraisnghamin operate in very different ways. For example, Fahlman discusses replacing sensitive textual information with tokens such that a sanitized message may be handled by intermediate processing, such as human-assisted translation (*see e.g.*, column 4, lines 60 - 66 of Fahlman) whereas Thuraisnghamin stores information on a database in a manner that prevents unauthorized disclosure to accessing users. One skilled in the art would not be motivated to combine the teachings of Fahlman and Thuraisnghamin because they attempt to solve different problems. Fahlman addresses how to ***transmit*** modified information to an intermediate service provider who is not authorized to receive sensitive information. Thuraisnghamin is directed to securing a database against ***access*** initiated by unauthorized persons. Not only is there no reasonable suggestion or motivation to combine reference teachings, there is also no reasonable expectation of success in the combination. It is unclear how the combination proposed by the Examiner would function. If Fahlman was modified to require the recipient to login as in Thuraisnghamin, that would fundamentally contradict the teachings of Fahlman that require "pushing" of messages to the intermediate service provider.

Moreover, if such a login was implemented in Fahlman, it is unclear how access would be limited to include the information that Fahlman wishes to provide to the intermediate service provider but not include sensitive information (that Fahlman replaces with tokens when transmitted). Since one skilled in the art would not be motivated to combine Thuraisnghamin with Fahlman and because it is entirely likely that the proposed combination would fail, the Applicant maintains that Claim 13 is novel and non obvious in view of the cited references.

Regardless, neither Fahlman nor Thuraisnghamin teach or reasonably suggest, either alone or in combination, operating a computer-based sanitization tool for sanitizing a received message to generate first and second sanitized messages that differ based on respective first and second security levels. Nor do they teach first and second sanitized messages. Accordingly, the cited references do not teach all of the Applicant's claim elements as required. Accordingly, the Applicant maintains that Claim 13 is novel and non obvious in view of the cited references. For at least the reasons cited herein, the Applicant maintains that Claim 13 is in condition for allowance and respectfully requests such disposition.

Claims 14 – 20 depend from independent Claim 13 and inherit all of the novel and non obvious features of the independent claim. For example, in Claim 17, the Applicant recites that the message includes a graphics portion and the step of third operating comprises protecting sensitive information within the graphics portion such that the sensitive information is not usable by the first recipient. The Examiner states that Fahlman teaches such at column 4, lines 22 - 26 and 47 - 53. Here, Fahlman states that a sender can compose an original message which can subsequently have sensitive information removed. Fahlman merely references videotaping but does not state how it is performed. All that Fahlman teaches is with respect to removing sensitive text from a text message. Unlike Fahlman, the Applicant claims a step of protecting sensitive information within a graphics portion that is fully supported on pages 19 and 20 of the present application. For at least these reasons, Claim 17 is novel and non obvious in view of the cited reference.

In another example of the patentable features of the Applicant's claims, the Applicant recites in Claim 18 that the step of third operating includes parsing the message into a number of tokens and separately analyzing each token for sensitive information. The Examiner states that Fahlman teaches such at column 4, lines 37 - 45. Hear Fahlman discusses the replacement of sensitive information with tokens. This differs from the Applicant's claims because, among other reasons, Fahlman is not first parsing the message into a number of tokens and then analyzing those tokens for sensitive information. Rather, Fahlman first analyzes the message for sensitive information and then replaces that sensitive information with tokens. Because Fahlman does not teach or reasonably suggest that which the Applicant claims in Claim 18, Claim 18 is patentable in view of the cited references.

In Claim 19, the Applicant recites that the step of third operating includes identifying a first format associated with the first potential recipients and converting the first sanitized message into the first format. Claim 19 also requires that the step of fourth operating includes identifying a second format associated with the second potential recipient and converting the second sanitized message into the second format. The Examiner states that such is taught in column 3, lines 56 - 60, column 4, lines 64 - 65, and column 5, lines 1 - 17 of Fahlman. Here, Fahlman merely teaches stripping a message of sensitive terms and replacing those terms with tokens. The sensitive terms are stored with mapping information such that the sensitive terms may be replaced after intermediate processing (e.g., translation) is performed. However, Fahlman does not teach converting a first sanitized message into a first format and a second sanitized message into a second format. Even if the subsequent replacement of tokens with sensitive terms were to be construed as formatting, Fahlman does not teach or reasonably suggest multiple formats for sanitized messages. Moreover, Fahlman does not even use the word "format" once in the entire patent. Accordingly, Fahlman does not teach or reasonably suggest that which the Applicant claims. For at least these reasons, the Applicant respectfully requests reconsideration and allowance of Claim 19.

Claim 20 recites a step of providing storage including first specification information for the first format and second specification information for the second format, wherein the step of third operating comprises accessing the storage to obtain the first specification information and the step of fourth operating comprises accessing the storage to obtain the second specification information, wherein the storage can be used to reconfigure the sanitization tool for transmission in multiple formats without re-compiling. The Examiner states that such is taught in Fahlman at column 2, lines 43 - 56. Since Claim 20 also recites formatting of sanitized messages, similar arguments may also be used here. However, Claim 20 also requires accessing storage to obtain the first and second specification information. Fahlman does not teach or reasonably suggest, either alone, or in combination with Thuraisnghamin, storage that can be used to reconfigure the sanitization tool for transmission in multiple formats without re-compiling. For at least these reasons, Claim 20 is also novel and nonobvious in view of the cited references. The Applicant respectfully requests reconsideration and allowance of Claim 20.

<u>Claim 30</u>

In Claim 30, the Applicant recites a method for use in a multi-level secure system for sanitizing a message. The method includes the steps of receiving an input file that includes information associated with at least first and second security levels of the multi-level secure system, wherein a user associated with the first security level of the multi-level secure system is entitled to receive information that a user associated with the second security level of the multi-level secure system is not entitled to receive, determining a security level associated with at least one user of the multi-level secure system to be the second security level and parsing intelligible elements from the information of the input file. The method also includes the steps of analyzing the intelligible elements to select a portion of the intelligible elements for sanitization according to the second security level, sanitizing the information of the selected portion of the intelligible elements according to the second security level to generate an output file for the at least one user of the multi-level secure system, wherein the output file has a first format. Additionally, the method includes the steps of formatting the output file to a second format for the at least one user of the multi-level secure system and transferring the output file in the second format to the at least one user of the multi-level secure system.

Claim 30 is patentable because, among other reasons, Thuraisnghamin does not teach either parsing or formatting and Fahlman does nothing to supplement Thuraisnghamin in this regard as the Examiner suggests. For example, parsing intelligible elements generally regards determining various informational components of a file. The Examiner states that Fahlman teaches such at column 4, lines 20 - 29. Here, Fahlman simply searches for sensitive terms and replaces those terms with tokens. The Applicant's claims are more analogous to that discussed in the arguments for patentability of Claim 18. That is, Fahlman differs from the Claim 30 because, among other reasons, Fahlman does not first parse a message and then analyze the parsed intelligible elements. Rather, Fahlman first analyzes the message for sensitive information and then replaces that sensitive information with tokens.

Fahlman pedantically searches for sensitive terms in a file (e.g., a person’s name and address in a letter). *See e.g.*, column 5, line 40 – column 6, line 20. The Applicant's invention relates to an algorithmic process for determining all intelligible elements generally without regard to the file type wherein each intelligible element in the file receives a token - not just the sensitive words like Fahlman teaches. The Applicant's claimed process is far superior because it has the ability to recognize intelligible elements (e.g., text, graphics, and sounds) and then determine whether or not to sanitize them. While Fahlman's teachings differ from the Applicant's Claim 30, Thuraisnghamin does nothing to supplement Fahlman in this regard. Accordingly, Claim 30 is patentable and the Applicant respectfully requests such disposition.

Additionally, the Applicant recites steps of sanitizing the information of the selected portion of the intelligible elements according to the second security level to generate an output file (i.e., having a first format) for the user of the multi-level secure system and formatting the output file to a second format for the user of the system. The Examiner states that such is taught in column 4, lines 42 - 66 of Fahlman. Again, Fahlman merely teaches stripping a message of sensitive terms and replacing those terms with tokens at this reference. The sensitive terms are stored with mapping information such that the sensitive terms may be replaced after intermediate processing (e.g., translation) is performed. However, Fahlman does not teach the formatting of the Applicant's claims. Accordingly, Fahlman does not teach or reasonably suggest that which the Applicant claims. Thuraisnghamin does not supplement Fahlman in this regard because these references are not properly combinable for reasons set forth above. For at least these reasons, the Applicant maintains that Claim 30 is patentable and respectfully requests such disposition.

Claim 31

In new Claim 31, the Applicant recites method for use in a multi-level secure system for sanitizing a message. The method includes a step of establishing rules based logic for use in determining a level of access to sensitive information as a function of information regarding an intended recipient of a message including at least a portion of the to sensitive information, wherein different recipients are associated with different levels of access to the sensitive information, the rules based logic further being operative for analyzing specific items of the sensitive information in the context of a given message relative to a selected rule set of a number of rule sets, wherein different ones of the rule sets correspond to set different levels of access to the sensitive information. The method also includes steps of receiving, in a processing system including the rules based logic, a first message including a first item of the sensitive information, analyzing, in the processing system, the first message to obtain recipient information regarding a first intended recipient of the first message, and based on the recipient information, accessing a first rule of a first rule set of the number of rule sets using the processing system. Additionally, the method includes steps of applying the first rule to process the first item of sensitive information, using the processing system, so as to generate a processed first message having a difference in relation to the first message, the difference being a function of the recipient information regarding the first intended recipient and operating the processing system to cause the processed first message to be transmitted to the first intended recipient.

Neither Fahlman nor Thuraisnghamin teach or reasonably suggest such a method, either alone or in combination. For example, the method recites different recipients that are associated with different levels of access to sensitive information. Thuraisnghamin is more analogous to users accessing a database as opposed to users receiving information. The claimed recipients are generally identified based on their various levels of access whereas Thuraisnghamin classifies data within a database without regard to individual recipients. Fahlman does nothing to supplement Thuraisnghamin in this regard because Fahlman removes sensitive terms from an original message to send the message to intermediate processing (e.g., human-assisted translation) such that the processed message can be later combined with the previously removed sensitive terms. More simply, Fahlman does not use a database for users to access. Additionally, Fahlman's method is less effective than the Applicant's claims because, among other reasons, Fahlman's method inefficiently scans a document for sensitive terms such that the intermediate processing does not see the sensitive terms in the document only to have those sensitive terms recombined with the document for viewing by a recipient. The Applicant's claimed invention, on the other hand, sanitizes sensitive terms based on different levels of access. In this regard, a single original message may be able to produce sanitized messages that differ but may be transmitted simultaneously (i.e., to different recipients). For at least these reasons, Claim 31 is patentable in view of the cited references.

The Applicant has also added new Claims 32 – 34. While these claims depend from new independent Claim 31 and, therefore, inherit all of the novel and non obvious features of the independent claim, these claims require additional features. For example, in Claim 32, the Applicant recites that the method further includes processing the first item of sensitive information according to the first rule, wherein the processing includes altering the first item of sensitive information or removing the first item of sensitive information. Fahlman does not teach a process which either removes or otherwise alters a sensitive term. For example, the identified sensitive term may be alternatively encrypted according to the Applicant's claims but Fahlman does not teach such an option. Fahlman, therefore, does not teach or reasonably suggest that which the Applicant claims.

In Claim 33, the Applicant recites that the method further includes processing the first message according to a second rule associated with a second recipient to generate a second message that differs from the first message. In Claim 34, the Applicant recites that processing the first message includes processing a second item of sensitive information according to the second rule, wherein the processing the second item of sensitive information includes altering the second item of sensitive information or removing the second item of sensitive information. Fahlman does not teach or reasonably suggest generating a second message from a first message in which sensitive terms are either removed or otherwise altered. Rather, Fahlman teaches generating a sanitized message which is recombined with sensitive information. That is, if the sanitized message was even construed as the Applicant’s claimed second message, the Applicant’s claims require removal or altering of additional sensitive terms in the second message. Fahlman, on the other hand, recombines the sensitive terms with the sanitized message. Accordingly, Fahlman does not teach a reasonably or suggest that which the Applicant claims. Nor does Thuraisnghamin supplement Fahlman in anyway because, among other reasons, Thuraisnghamin is directed to preventing unauthorized access to a database as opposed to sanitizing messages. For at least the reasons cited hereinabove, the Applicant maintains that Claims 32 - 34 are also patentable.

CONCLUSION

Based upon the foregoing, the Applicant believes that all pending claims are in condition for allowance and such disposition is respectfully requested. In the event that a telephone conversation would further prosecution and/or expedite allowance, the Examiner is invited to contact the undersigned.

Respectfully submitted,

MARSH FISCHMANN & BREYFOGLE LLP

By: /Gregory T. Fettig/
Gregory T. Fettig
Registration No. 50,843
3151 South Vaughn Way, Suite 411
Aurora, Colorado 80014
Telephone: 720-562-5509

Date: October 2, 2006